How much cash is in crypto?

Beat Weber[1]
Refereed by: Rainer Böhme, University of Innsbruck

In 2008, an anonymous white paper introduced "bitcoin." Its ideas triggered and inspired the emergence of thousands of crypto assets in its wake. Putting key terms used in this paper to a close reading reveals that terms like "electronic cash," "peer-to-peer" and "inflation" are used in a different sense than is customary in economic debate. Despite claims put forth in the white paper, transferring bitcoins is neither "peer-to-peer" in the sense of a non-intermediated transfer between two individuals nor does bitcoin offer technical protection against losses in value and is therefore not "inflation free." Last but not least, bitcoin is not a carrier of stable value that is generally accepted like cash.

JEL classification: E42, E52, E58
Keywords: crypto assets, cash

From bitcoin to crypto assets: looking for a place in the world of economic value

If all owners of crypto assets of any type had found buyers for their holdings in exchange for cash when the 2021 rally on crypto markets peaked in November, as much as EUR 2.5 trillion would have changed hands. At the time of writing in January 2022, it would have been EUR 1.4 trillion.[2] In contrast to cash stored in safe-deposit boxes at banks and bank deposits that represent claims on banks to provide cash on demand at par value, the relationship between crypto assets and cash is characterized by considerable uncertainty.

More than a decade after the publication of the initial paper "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, 2008), the answer to the question what bitcoin or similar crypto projects are still depends on who you ask and where you look: white papers written by developers, marketing messages of crypto businesses, user surveys, academic research, policymakers or legal texts, etc.[3]

Depending on who you ask, you will find that different terms are used to describe the same crypto phenomena and that terms may mean different things when related to classifying and describing crypto projects.[4]

Therefore, we should take a closer look at the terminology: what do key terms widely used by crypto enthusiasts to describe the properties of bitcoin and similar projects actually mean? What do expressions like "peer-to-peer electronic cash" that is "inflation free" refer to in an economic sense? Are there ambivalences in meaning which might be noteworthy or even misleading?

[1] *Oesterreichische Nationalbank, EU and International Affairs Division, beat.weber@oenb.at.* *Opinions expressed by the authors of studies do not necessarily reflect the official viewpoint of the OeNB.* *The author is grateful to Rainer Böhme, Ingrid Haussteiner and Martin Summer for very helpful comments.*

[2] *https://coinmarketcap.com/de/charts/.*

[3] *For a discussion of other crypto-related aspects in previous issues of this journal, see Beer and Weber (2014) and Pichler et al. (2018).*

[4] *See Financial Times (2021). Even to use the term "crypto" as a catch-all term for all projects in the wake of bitcoin is a contestable form of borrowing a shorthand for the term "cryptography" to denote what European legislators call "crypto assets."*

The brainchild of an anonymous entity (Nakamoto, 2008), bitcoin came into being in 2008. From the beginning, it has attracted people that attach meaning and devote time and resources to it. Also, bitcoin has triggered various forms of economic activity, and it has inspired the creation of thousands of additional crypto projects. With the regulation on markets in crypto assets (MiCA),[5] the EU is about to establish a comprehensive set of laws applicable to crypto-related activities. Importantly, the regulation is expected to help clarify the relation of crypto phenomena to legal concepts as well as the legal rights and duties attached to them. A major step for both legal systems and crypto-related activities, this legislation is likely to have a decisive influence on the economic activities related to crypto projects. After all, the legal system plays a key role for the operation of the economic system (Pistor, 2019). Note that the MiCa draft refers to "crypto assets" in its title instead of the more popular term "cryptocurrencies." This illustrates that integrating innovation into existing legal and economic systems can also imply confrontation with existing classification systems that exert terminological adjustment pressure.

Bitcoin is the most spectacular attempt in recent history to translate cash into electronic form. In describing this attempt, the pseudonymous author(s) of the initial white paper and subsequent presentations make(s) use of several terms, definitions and descriptions from the English language that give people tools to make sense of this novel concept. Based on this, other people have been devoting attention, interpretations, time and resources to this concept, giving it a social existence.[6]

One starting point for exploring the sources of views, interpretations and labeling efforts with regard to crypto projects is to investigate the context from which bitcoin originated. This context has political aspects: bitcoin emerged from discussions in the "cypherpunk" community. Its members develop privacy-enhancing tools to promote a society characterized by "crypto anarchy." Cypherpunk is a variant of a techno-political view of the internet as a new form of society where freedom means markets and money beyond law, politics and parliamentary democracy (Brunton, 2019; Clark, 2016). The global financial crisis from 2007 to 2009 has significantly influenced the economic context, focusing public attention on issues related to money and finance, government and banking. Another contextual aspect is the field of expertise the developers of bitcoin come from. As a major early survey on the phenomenon notes, "bitcoin's rules were designed by engineers with no apparent influence from lawyers or regulators" (Böhme et al., 2015, p. 213).

Why would identifying crypto designers' field of expertise matter for discussing the nature of bitcoin or crypto assets in general? For one thing, fields of expertise are intertwined with specific world views, among other things. For another, experts usually develop specific terminologies, where terms are given clearly defined meanings fit for their context. We know this from fields like engineering, law or economics, each of which may be further divided into subfields such as game theory and monetary economics as well as different schools of thought, etc. Also, different fields of expertise may use the same terms with different definitions. This

[5] *For a draft, see European Commission (2020).*

[6] *Shiller (2020) highlights the role of sense-making in the form of narratives for economic activity, including bitcoin. Hasufly and Carter (2018) survey key narratives around bitcoin.*

may lead to misunderstandings among members of different fields of expertise, specifically when there is a lack of time, awareness or intention to spell out and discuss the precise meaning and implications of terms.

Böhme et al. (2015) give a further clue on the engineering perspective informing bitcoin by characterizing the project as "an online communication protocol that facilitates the use of a virtual currency." Highlighting the communication aspect is relevant because money, e.g. banknotes, coins, bank deposits or e-money, transferable on payment systems is a means to communicate about economic value, with money serving as a kind of language for the economic system. Any design of money therefore requires consideration of a mechanism that makes money represent economic value and how such money can be used in the economy it is intended for.

In engineering and engineering theory, however, communication is studied in a narrow sense – as the technical process of signal transmission. Hence, engineers treat signals as a physical phenomenon, quantitatively measured in bits. On this conceptual basis, engineering inquiries measure and compare the effort and capacity of various channels for the undistorted technical transmission of signals in various forms. In contrast, the processes associated with coding and decoding social meaning to be transported in communication do not form part of the analysis (Eco, 1976; Shannon, 1948).

While the social – including the economic – dimension and meaning of communication are usually not part of the engineering discipline, the white paper on bitcoin and many references to bitcoin lack such a clarification. As a result, interpretations give rise to ambiguities.

So, how does the white paper on bitcoin use and define key terms that have over time become prevalent in debates about crypto assets and their relation to cash? In a community heralding its dislike of authority, the white paper is perhaps the closest equivalent to something like a foundational text. The fact that the author or authors chose to publish the text under the pseudonym "Satoshi Nakamoto" may have helped avoid personal disputes inventors are often faced with. Most people associated with bitcoin would probably agree on the document's relevance and influence. Although the text and its concept are subject to many disagreements, many terms as used and defined in the bitcoin white paper have been widely adopted among crypto supporters. Among thousands of crypto assets, bitcoin is still the most widely known and by far the biggest one, accounting for a share of around 40% in widely used metrics of crypto market value.[7]

A close reading of the meaning of key terms used in the white paper could therefore be a useful contribution to the wider debate on what bitcoin-like crypto projects are and how they resemble – or differ from – existing economic phenomena like official currency. In the following, I discuss three key terms particularly relevant to comparing crypto assets like bitcoin with banknotes and coins in official currency: (1) cash, (2) peer-to-peer, and (3) inflation. There are many other terms which are widely used to describe or promote bitcoin-like projects, e.g. "cryptocurrency," "token" or "payment system." Here, I concentrate on the term "cash" because this publication centers on this specific form of money. "Peer-to-peer" is the most specific form of what bitcoin supporters perceive as bitcoin's distinctive

[7] *https://www.statista.com/statistics/1269302/crypto-market-share/*.

organizational feature compared to official currency: decentralization. Finally, "inflation" is a key term in any discussion on the economic value of money.

The annex provides a short glossary defining six terms widely used in the context of crypto assets.

1 "Cash"

In the title of the 2008 white paper, bitcoin is introduced as an "electronic cash system." From this starting point, the paper (Nakamoto, 2008, p. 2) then proceeds to define the more specific term "coin": "We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership. " In the rest of the paper, "coin" is used as a suffix in the project's name, bitcoin, and as a term to describe the units of value its protocol aims to create.

According to this definition, bitcoins are chains of digital signatures. These signatures form part of a database ("blockchain"). And this blockchain is administered by a computer network subject to rules and incentives defined in a protocol. With the exception of node activity expending central processing unit (CPU) time and energy required for creating and ensuring access to them, coins as described in the white paper do not contain any reference or connection to any economic phenomena or entities[8] outside the database: the signatures constituting "coins" refer only to each other. After being created through "mining" activity, access to "coins" can be transferred among unidentified users on a voluntary basis.

How does this compare to characteristics of cash in the traditional sense? In monetary systems based on official currencies, signatures also play a role. One role is to identify, via handwritten signatures or PIN codes, owners willing to access funds held in bank accounts or provided by credit card schemes at physical points of interaction. A similar function is attributed to the mechanism to give access to "coins" in bitcoin where owners electronically sign funds.[9]

But more importantly, signatures also play a key role for transforming physical objects into cash for use in an economic context. The signature of (central) bank representatives on banknotes is a key aspect of what distinguishes cash from a mere assembly of pieces of printed paper (or, in the case of coins, metal) in limited quantity. Signatures on banknotes signify that an issuing bank assumes liability for its notes. In the current monetary systems, central banks are the sole issuers of banknotes in official currency in most jurisdictions. From the perspective of the issuing central bank, this means that issued notes represent liabilities for the central bank. Beyond the mere printing, issuing notes requires a counterparty willing and able to acquire new notes in exchange either for a collateralized claim on the counterparty or for securities issued by third parties (e.g. government or corporate bills and bonds).[10] Assets received in exchange for new notes are subsequently held

[8] *For instance issuers, persons, goods and services, claims or assets.*

[9] *A major contrast to bank accounts is that bitcoin's protocol design makes it technically possible for individual bitcoin owners not to disclose their identity to a third party, but the blockchain contains a complete public register of every bitcoin transaction ever made.*

[10] *See Bindseil (2004), DNB (2015) and ING (2018) on money's operational details.*

on the central bank's balance sheet to back its liabilities until the issuing of money is reversed at contract maturity. At maturity date, debtors have to pay central bank money to the central bank, returning money to the issuer after circulation. By accepting its own liabilities (either electronic reserves or banknotes) at face value to extinguish liabilities of its debtors, the central bank redeems its own liabilities.[11] When counterparties pay debt held by the central bank, both the money returning to the central bank and their own liabilities are extinguished. Because central bank liabilities in the form of banknotes do not offer interest, positive returns accruing on assets held by the central bank as counterparts to circulating banknotes (and electronic reserves) represent income to the central bank ("seigniorage").

From the perspective of central banks' counterparties (i.e. mainly commercial banks in most jurisdictions), holding banknotes means having a claim on the central bank that is received in exchange for an asset (securities held by banks) or incurring a liability to the central bank. By granting credit to bank customers and by accepting cash deposits, commercial banks themselves incur liabilities to their customers. Access to cash for users in the general public is intermediated via the banking system. Cash users are not interested in redeeming banknotes at the central bank to reduce corporate or public debt held by the central bank. Instead, they use money to pay and compare prices of goods and services, or store value.

Bank customers among the general public can use deposits with commercial banks to hold funds denominated in official currency, to make payments by instructing banks to transfer funds to other bank customers, or to withdraw cash at par value on demand. When bank customers make payments by bank transfer across banks, banks settle these payments by transferring central bank reserves among themselves.

Individual banknotes, coins and bank deposits in official currency form both a part of their own class (a numbered series of banknotes, a stock of coins, a stock of deposits, statistically measurable at any point of time as components of the money supply in an economy) and a key part of a chain of contractual commitments across the whole economy.

Because credit is a key input in financing the flow of production of new goods, services and assets, production of money for the economy by providing credit is directly connected and integral to the rest of the economic system. That is why cash or electronic forms of payment in official currency are not just a chain of signatures that give access to a limited stock of monetary objects, but a chain of signatures that represent and form part of a chain of claims across the whole economy that includes the issuer, its counterparties from the financial sector and various entities from the private and public sector engaging in economic activity. Being part of a pervasive chain of claims that are constantly confirmed by money payments when due, money in official currency can come to be treated as if it were a direct claim on any good, service or asset available in markets within the currency area concerned. This is supported by its exclusive acceptance for tax payment purposes and by legal tender laws making it the standard means of payment.

Unlike vague promises, these commitments are quantified and obtain their credibility from the fact that they are costly to break because of incentives and sanctions provided by legal, economic and political systems which they form part of.

[11] *For a practical illustration of key aspects of these mechanisms, see Koning (2021).*

In contrast, the signatures of which bitcoin consists of (i.e. each bitcoin amount consists of a unique pair of a private and a public key) are only a technical tool to provide access to electronic coins, provided the system operates in line with its description, with no references implied to the outside world. There is no reason for users to treat such coins as if they were a direct claim on any good, service or asset available in markets. Over time, bitcoin and similar crypto assets have found a market that initially emerged from, and continues to follow, the logic of markets for collector items: information on limited supply in combination with an intriguing narrative meets unpredictable demand, which results in an unpredictable market price over time.[12] The role of crypto assets for payments has been limited to small niches where payment in official currency is not possible or desired, with prices of goods and services determined in official currency. Their main resemblance to official currencies is the part of activity that is observable in foreign exchange trading markets, whereas the role of official currencies in serving as a stable unit of account, generally accepted means of payment and most liquid store of value within their domestic economy has not been replicated by bitcoin and similar crypto assets (Makarov and Schoar, 2021).

Whereas other projects in the wake of bitcoin have continued to use the term "cash" in a similar sense (e.g. "Dash," "Zcash," or "BitcoinCash"), the most pervasive and most telling use of the term in current crypto-related activity is the phrase "to cash out."[13] In contrast to identifying crypto itself as a form of cash, this phrase describes how crypto assets only result in cash when crypto funds are converted into official currency. The main use of bitcoin and similar crypto assets is in their being held and traded with a view to expected changes in their market price as measured in official currency (Makarov and Schoar, 2021). Therefore, most users are more interested in being able to convert crypto assets into traditional forms of cash than in using crypto assets in lieu of cash to make payments or in using them as a yardstick to measure the value of goods.[14]

Crypto users' need to "cash out" on demand has given rise to "stablecoins" (ECB, 2021). Both the contemporary significance of stablecoins for crypto-related economic activity and their construction are a disappointment to anybody who expected bitcoin and similar crypto assets to rival or replace cash and other forms of official currency.

In contrast to bitcoin's conceptualization of coins as chains of signatures that refer only to their own database, stablecoins are constructed in a way resembling more closely that of actual cash or bank deposits: they have an issuing entity that proclaims to back "coins" by marketable assets held by the issuing entity. Stablecoins are available to users in exchange against official currency. Most stablecoins

[12] *In an e-mail, replying to a suggestion to compare bitcoin to shares, Nakamoto (2010) writes, "bitcoins have no dividend or potential future dividend, therefore not like a stock. More like a collectible or commodity." In line with this classification, the earliest significant trading platform for crypto assets was Mt.Gox (short for "Magic: The Gathering Online eXchange"). The platform started as a venue for trading collector cards from the fantasy game of the same name, before introducing bitcoin trading facilities in 2010 and becoming the world's leading bitcoin exchange until its spectacular crash and bankruptcy in 2014 (McMillan, 2014).*
In recent years, the hype created by crypto projects dedicated to the deliberate creation of collector items void of other economic ambitions like CryptoKitties and nonfungible tokens (NFTs) has served to underline the continued relevance of collector market mechanisms to understand the crypto sector.

[13] *See e.g. information provided by two large global crypto trading sites: Binance (2021) and Coinbase (2022).*

[14] *FCA (2021), Makarov and Schoar (2021).*

attempt to relate their value at par to the US dollar or other major official currencies. This mechanism is intended to produce stability in terms of stable market value of these coins against official currency, similar to a bank deposit that is exchangeable on demand with cash at par value. Stablecoins currently serve as a kind of shadow banking system for the crypto sector: they are used for storing and transferring funds in relation to crypto trading in cases where there are legal or economic constraints (e.g. know your customer and anti-money laundering (KYC/AML) requirements, lack of connection of decentralized exchanges to conventional payment systems) to accessing bank deposits for these activities.

Regulatory frameworks for stablecoins are expected to be decisive for whether and how stablecoins can maintain, modify or even expand their role beyond crypto asset trading. So far the role of stablecoins has confirmed the unchanged importance of the world's key currencies as stable anchors of value even in the niches of economic activity related to crypto assets.

2 "Peer-to-peer"

A key attribute often held to characterize bitcoin and similar projects is the alleged absence of intermediaries. According to evidence from e-mails and the protocol code, white paper author Nakamoto's dislike of intermediaries results from an affinity to monetary reform ideas inspired by a commodity view of money, where the role of money is thought to be subject to some kind of natural laws (Mehrling, 2017; Weber, 2018). These aspects are not stressed in the white paper, however. Instead, granting that the current system "works well enough for most transactions," Nakamoto (2008, p. 1) cites costs and privacy issues associated with fraud prevention in intermediated electronic payments as a problem which bitcoin seeks to address. It does so by attempting to replace the need for trusted third parties.

In the bitcoin white paper, the term "peer-to-peer" (P2P) is already part of the title ("Bitcoin: A Peer-to-Peer Electronic Cash System"). The paper's abstract specifies that "We propose a solution to the double spending problem using a peer-to-peer distributed time-stamp server to generate computational proof of the chronological order of transactions" (Nakamoto, 2008, p. 1).

In the paper, the "double spending problem" (resulting from the possibility for any user of easily copying electronic coins like other forms of digital content online, thereby increasing one's funds with minimal effort) is described as follows: "[…] the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. […] To accomplish this without a trusted party, transactions must be publicly announced, and we need a system for participants to agree on a single history of the order in which they were received" (Nakamoto, 2008, p. 2). After describing key elements of the protocol, the paper concludes: "We have proposed a system for electronic transactions without relying on trust. […] a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power" (Nakamoto, 2008, p. 8).

In an e-mail accompanying the introduction of bitcoin, the author(s) add(s): "The result is a distributed system with no single point of failure. Users hold the crypto keys to their own money and transact directly with each other, with the help of the P2P network to check for double-spending" (Nakamoto, 2009).

What does this mean? In the technical sense used in the white paper, "peers" consist of computers, and the term "peer-to-peer" describes a relation among computers in a network. In contrast to a hierarchical client-server relation, a peer-to-peer computer network consists of several independent machines that are equally eligible to share in contributing to a particular task or function.

In a social and economic sense, however, the term "peer" refers to an individual, and the term "peer-to-peer" describes a direct relation between individuals. As defined in Investopedia (2021), "A peer-to-peer (P2P) economy is a decentralized model whereby two individuals interact to buy/sell goods and services directly with each other or produce goods and service together, without an intermediary third-party or the use of an incorporated entity or business firm."[15]

While the term "peer-to-peer" is mainly used in a technical sense by the author(s) in the bitcoin white paper, and the latter concentrates on outlining its technical consequences in the context of the protocol (control of double spending, no single point of failure), on some occasions it does not take that much care to prevent a reader from giving it a social interpretation: "users [...] transact directly with each other," "a system for electronic transactions without relying on trust," "without a trusted party," "allowing any two willing parties to transact directly with each other without the need for a trusted third party" (see Nakamoto quotes cited above).

Whatever the intention of the white paper's author(s), the use of the term P2P in the bitcoin white paper has nurtured optimism among some of its readers that the intermediaries' role in money and economic activity can be removed with the help of bitcoin and other technological innovations based on blockchain technology (Berg et al., 2019).

But irrespective of the state of technology, intermediaries are key to money and market exchange in modern economies for economic reasons.

Before an exchange can take place, even if we envisage the possibility of a direct bilateral exchange of good against good, some common ground must be established among trading partners. If there is no inequality between the two goods (i.e. if the two are identical), an exchange will make no sense. If there is inequality between the two, some form of equality needs to be established, otherwise there will be no exchange (unless inequality among trading partners gives rise to forced or unequal exchanges). In developed market economies, prices of goods, services and assets are established in money (official currency) as the yardstick to measure value. Market prices are the reference against which exchange rates for goods (and services, and e.g. also assets) are established in a bilateral exchange. Organized markets in a developed economy intermediate bilateral trade by providing indispensable tools for the exchange, above all money, market prices denominated in official currency and a legal system that protects private property and enforces contracts.

In contrast to this, engaging in a non-intermediated bilateral barter exchange implies a lack (of awareness) of market prices, of alternative trading partners potentially offering better bargains and of the other abovementioned tools provided by modern markets. As illustrated in the famous fairy-tale recorded by the Brothers

[15] *See Mueller (2018) for a conceptual analysis of the notion of a peer-to-peer economy.*

Grimm "Hans in Luck" ("Hans im Glück" in the German original),[16] structural lack of intermediation in barter exchanges is likely to lead to unfavorable exchanges and can quickly end in ruin.

Not only do money and markets serve to intermediate economic exchanges, but money itself is also issued by a responsible intermediary. Having said this, a unique feature that distinguishes cash from electronic forms of money like bank deposits is that some – but not all – of its functionalities enable handling on a P2P basis.

Cash can change hands between two individuals without a third party having to be present, or to be aware of, provide input to, take note of or record the transfer. Physical cash is transferable on a peer-to-peer basis. Nevertheless, the existence of an intermediary responsible for issuing, backing and guaranteeing cash is indispensable for its functioning. Cash is much more than just an(y) object in limited quantity. The fact that cash can be exchanged between two individuals against objects traded on markets does not mean that we live in a peer-to-peer economy, where individuals can bilaterally regulate all aspects involved in the trade of objects and intermediaries are superfluous. Trades are typically intermediated by issuers of money guaranteeing its quality, payment service providers, markets providing reference prices for most products and services, a number of legal protections against fraud, theft and mistakes, marketplace providers like supermarkets, to name just some key intermediaries. The invention of crypto assets and technical architectures like blockchains does not replace these functions, and does not open a likely path into a "barter economy of the future" (Berg et al., 2019, pp. 74ff.).

Bitcoin-like crypto assets are not even P2P in the limited social sense the term applies to physical cash, and can hardly be expected to replace intermediaries in key areas of contemporary markets. Bitcoins are not transferable without a third party serving as an intermediary. But for performing some of the functions traditionally performed by intermediaries, bitcoin replaces responsible regulated entities (banks and other financial institutions competing on markets for users) with incentives to attract competing volunteers among users subject to market mechanisms. Among intermediation functions, the bitcoin protocol focuses on solutions for counterfeit control and validation of transactions. Users serving as "miners" by contributing computer power to the bitcoin network compete for new bitcoins by validating bitcoin payments between other users and checking against double spending of coins.

As a result of this design, transferring bitcoins to another user means having your transaction proposal intermediated, i.e. checked and confirmed by a third party in between. The fact that this third party consists of a network of computers belonging to competing firms and individuals operating under the incentives and constraints provided by the protocol surely makes a difference in terms of how this intermediation function is organized, in contrast to e.g. a bank or a traditional payment service provider network. It also makes a difference with respect to the range of services such an intermediary architecture can provide. Most importantly, whereas a regulated bank or card network guarantees the economic value of the

[16] *Starting off with a piece of gold, Hans makes several barter trades, always feeling lucky about them, and ends up with a grindstone and an ordinary stone – and ultimately with nothing, as the two stones finally fall into water.*

funds transferred and the legal finality of the payment, the only provision made in the bitcoin protocol to support the value of coins is the supply limit, which leaves it up to users to negotiate its value on markets not regulated by the protocol. But paying with bitcoins does not mean engaging in a non-intermediated transfer.

The competitive design of intermediation functions in bitcoin-like crypto assets has nurtured a further social interpretation of the notion P2P that has become popular in debates about crypto. This involves translating technical decentralization as political democratization. In this view, participation in the crypto ecosystem involves fairness and equality in the sense of open access and competition among individuals of equal power, in contrast to large traditional intermediaries enjoying considerable market power in the established economy. Therefore, some observers consider the technical decentralization in bitcoin-like architectures to be decentralization in the sense of dissolving social power, even a form of "democracy."[17]

Researchers have pointed out that it is questionable to apply the term "peer-to-peer" in this wider, more social sense for describing bitcoin's technical architecture given considerable market concentration in a number of key activities, i.e. mining, coding, ledger storing, coin ownership and the widespread use and market power of various intermediary services for trading, storing and transferring crypto assets (Makarov and Schoar, 2021; Walch, 2021). Although not directly subject to the bitcoin protocol outlined by Nakamoto, an ecosystem of crypto intermediary services has developed that is indispensable for the actual operation of crypto on its current scale. Sizable firms dominate the market of crypto exchanges, where users trade cryptos against official currency, publishing exchange rates serving as a reference for bitcoin's market value. Wallet providers offer services to safely store private keys giving access to bitcoins. Payment service providers offer to ease usability and absorb some risks associated with crypto payments. Many of these providers closely resemble traditional financial intermediaries.

The fact that bitcoin transfers are intermediated is also visible in the variable fees that providers of intermediary functions (i.e. successful miners) receive from users for confirming transactions. A peculiar aspect of bitcoin's design is that user fees do not absorb the full cost resulting from miners' transaction confirmation activity. Miners have to cover the rest of their substantial energy and computer costs by "cashing out," i.e. by selling new bitcoins created and received as a reward as intended by the protocol. In this way, people that buy new bitcoins on trading platforms subsidize existing users' transactions.

"Peer-to-peer" in bitcoin does not even mean the ability to transfer bitcoins between two individuals without support of a third party, which is possible with physical cash in official currency. In many areas of crypto markets, concentration and asymmetries of power are prevalent, which makes it hard to characterize the ecosystem as peer-to-peer based in a social sense.

3 "Inflation"

As mentioned above, the white paper on bitcoin does not discuss mechanisms how cash becomes a carrier of value. A key term used in discussing the economic value of money is "inflation." In a contemporary economic context, "inflation" means changes in the purchasing power of money as measured by changes in prices of a

[17] *See e.g. Mueller (2018) and Parkin (2019) for a discussion.*

basket of goods and services over a predefined period. Legal mandates for most central banks provide "inflation targets" in this sense of the term. Statistical agencies collect and publish statistical information about price changes in the economy, and policymakers use these and other sources of information to monitor the evolution of prices and instruments at their disposal to stabilize inflation.

In the white paper, the term "inflation" is mentioned only once: "By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. [...] Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free." (Nakamoto, 2008, p. 4).

Inflation in an economic sense is measured in the amount of goods and services a monetary unit is able to buy. In the bitcoin context, it is used in a different (more colloquial, metaphorical, or general) sense of "quantitative growth of a stock of items": inflation is defined self-referentially as growth of a stock of units as measured in its own unit, and does not refer to changes in its economic value in terms of its exchange rate against goods and services.

Crypto enthusiasts have increasingly adopted the term "inflation" to describe growth in the supply of a certain type of coin. A prominent example is the white paper of Ethereum, the second largest project in the crypto market of recent years (Ethereum, 2022).

Using the term inflation in the sense of "growth of the money supply" echoes a period in the 18th and 19th centuries when that was common among early scholars of the modern discipline of economics. While there is no consensus in contemporary research on causal relations between changes in the supply of money and the price level, analytical efforts to identify changes in the money supply as the key driver for changes in the price level persist, known as the "quantity theory of money" (Blaug, 1995). This theory presupposes several quantifiable and observable regularities in the role and usage of a clearly defined money supply in a clearly defined economy that demands and uses this supply.

But in the absence of any information on an economy that routinely uses a stock of units for a specific purpose, there is no way to derive the economic value, or changes of value over time, of such units from changes in their quantity. If you are asked to accept a payment of 1 bitcoin, technically verifiable knowledge that this represents 1 out of 21 million units is next to irrelevant for your decision. What counts is its economic value: what and how much you could obtain in exchange for 1 bitcoin (e.g. bread) and if such payment would be accepted. Unfortunately, if there existed a maximum output of e.g. 21 million loaves of bread on a given morning, this would not mean that 1 bitcoin would buy 1 loaf, even if you could be sure that bitcoins were accepted everywhere as a means of payment. Instead, markets coordinating supply and demand for each relevant unit or good (i.e. bitcoin and bread) determine the price of each and measure it in an external yardstick (in general an official currency). Comparing two items from different object classes based on the overall number of units available or any physical measure (like weight, size or temperature) does not offer any clue about the comparative market value of the two items.

The emergence of thousands of other crypto assets after bitcoin, some of them very similar to the original, provides a useful illustration. Like bitcoin, many of these assets are expected by their supporters to have functionalities close to money. Together, they provide millions of units, each potentially serving as money in markets for existing goods and services. If the mere coming into being of additional units of potential money led to inflation in the economic sense, the proliferation of thousands of crypto assets without their own economy would undermine any initial intention of limiting the supply of bitcoins to prevent monetary inflation. Even if bitcoin were the only crypto asset and were to be adopted as the single currency of an economy, the following would hold: in a capitalist economy, where permanent change (e.g. production, competition, innovation) is a key characteristic, a currency based on an immutable stock of money would prove unsuitable to fulfill monetary functions.

Therefore, vendors that promote bitcoin and similar crypto projects by referring to their alleged quality of offering "inflation protection"[18] use these terms in a non-economic sense. They do not refer to any technical defense against losses in market value over time, but to an upper limit for the supply inscribed in bitcoin's protocol and to the presence of incentive mechanisms to deter changes to this limit.

The bottom line is that important information is lacking even if we were to employ the most basic theory of market value, according to which market value is a result of the interaction of supply and demand. There is no ex ante knowledge of the fraction of bitcoin's total supply that is put on sale at a given time by existing owners or of the quantity of demand on markets where crypto assets are traded. The future evolution of both quantities is by and large unpredictable. This will not – nor should it – deter any interested parties to make their own assumptions and predictions about the future of the crypto market. But it would be highly misleading to create the impression that bitcoin and similar crypto coins rely on a technological mechanism that prevents the occurrence of losses in their economic value over time.

4 Conclusions

In this paper, I have subjected key terms associated with bitcoin, most importantly "cash" as in "electronic cash," "peer-to-peer" and "inflation," to a close reading by examining their definitions in the original white paper on bitcoins entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, 2008). In addition, I have contrasted the way these concepts are used in the crypto world with their meaning in debates about economic phenomena. The analysis revealed that the differences in usage and meaning of key terms are likely to be attributable to the engineering perspective taken by the pseudonymous author(s) of the white paper and bitcoin's initial supporters. Pointing out these differences may help avoid misunderstandings among potential users or students of bitcoins and similar crypto assets.[19]

[18] *See e.g. Kraken (n.d.).*

[19] *Note that there is a large literature where other key crypto-related terms have been subjected to critical investigation. Such terms include, for instance, "trustlessness" (e.g. Bratspies, 2018; Vidan and Lehdonvirta, 2018) or "smart contracts" (e.g. Schuster, 2021).*

Transferring bitcoins is neither "peer-to-peer" in the sense of a non-intermediated transfer between two individuals, nor does it offer technical protection against losses in value, i.e. it is not inflation free. And bitcoin is not like cash in important respects. In bitcoin and other crypto asset schemes, an assembly of machines is instructed to transport computer bits irrespective of their meaning. With actual cash in official currency, people and machines "transport" banknotes and coins because cash serves as a carrier of stable value that is generally accepted. A focus on tangible objects and their physical qualities is insufficient to comprehend the key role of intermediaries in this process.

As a result, the relation between cash and bitcoin-like projects is likely to remain unstable and uncertain in many respects.

References

Beer, C. and B. Weber. 2014. Bitcoin – The Promise and Limits of Private Innovation in Monetary and Payment Systems. In: Monetary Policy & the Economy Q4/14. OeNB. 53–66.

Berg, C., S. Davidson and J. Potts. 2019. Understanding the Blockchain Economy: An Introduction to Institutional Cryptoeconomics. Cheltenham.

Binance. 2021. How to Sell Gaming NFTs & Cash Out Crypto Via Fiat. https://www.binance.com/en/blog/nft/how-to-sell-gaming-nfts--cash-out-crypto-via-fiat-421499824684903104.

Bindseil, U. 2004. Monetary policy implementation. Theory, past and present. Oxford.

Blaug, M. 1995. Why is the quantity theory of money the oldest surviving theory in economics? In: Blaug, M., W. Eltis, D. O'Brien, R. Skidelsky and D. Patinkin (eds.). The quantity theory of money. Edward Elgar Aldershot. 27–49.

Böhme, R., N. Christin, B. Edelman and T. Moore. 2015. Bitcoin: Economics, Technology, and Governance. In: Journal of Economic Perspectives 29/2. 213–238.

Bratspies, R. 2018. Cryptocurrency and the Myth of the Trustless Transaction. In: Michigan Technology Law Review 25/1. https://repository.law.umich.edu/mttlr/vol25/iss1/2/.

Brunton, F. 2019. Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency. Princeton UP.

Bryan, M. F. 1997. On the origin and evolution of the word inflation. Federal Reserve Bank of Cleveland. https://www.clevelandfed.org/en/newsroom-and-events/publications/economic-commentary/economic-commentary-archives/1997-economic-commentaries/ec-19971015-on-the-origin-and-evolution-of-the-word-inflation.aspx.

Clark, J. 2016. The Long Road to Bitcoin. Foreword In: Narayanan, A., J. Bonneau, E. Felten, A. Miller and S. Goldfeder. Bitcoin and cryptocurrency technology. A comprehensive introduction. Princeton UP. ix-xxvii.

Coinbase. 2022. How do I sell or cash out my digital currency. https://help.coinbase.com/en/coinbase/trading-and-funding/buying-selling-or-converting-crypto/how-do-i-sell-or-cash-out-my-digital-currency.

DNB – De Nederlandsche Bank. 2015. Central banks keep finger on money creation pulse. https://www.dnb.nl/en/news/news-and-archive/dnbulletin-2015/dnb325255.jsp.

ECB. 2021. The expanding functions and uses of stablecoins. Financial Stability Review. November. https://www.ecb.europa.eu/pub/financial-stability/fsr/focus/2021/html/ecb.fsrbox202111_04~-45293c08fc.en.html.

Eco, U. 1976. A Theory of Semiotics. Indiana UP.

Ethereum. 2022. Whitepaper. https://ethereum.org/en/whitepaper/#currency-and-issuance.

European Commission. 2020. Proposal for a Regulation on Markets in Crypto-assets, COM(2020) 593. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

FCA – UK Financial Conduct Authority. 2021. Cryptoasset consumer research 2021. https://www.fca.org.uk/publications/research/research-note-cryptoasset-consumer-research-2021.

Financial Times. 2021. UK advertising regulator issues rebukes to crypto industry. https://www.ft.com/content/b48040e5-d510-4ac8-9e6c-6af568e587ad.

FSB – Financial Stability Board. 2022. Assessment of Risks to Financial Stability from Crypto-assets. https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/.

Hasufly and N. Carter. 2018. Visions of Bitcoin. How major Bitcoin narratives changed over time. https://medium.com/@nic__carter/visions-of-bitcoin-4b7b7cbcd24c.

ING. 2018. The money creation paradox. https://think.ing.com/uploads/reports/Money_paradox2.pdf.

Investopedia. 2021. Peer-to-Peer (P2P) Economy. https://www.investopedia.com/terms/p/peer-topeer-p2p-economy.asp.

Koning, J. P. 2021. Is money a ponzi? http://jpkoning.blogspot.com/2021/12/is-money-ponzi.html.

Kraken. n.d. Bitcoin as a Hedge Against Inflation. https://www.kraken.com/learn/finance/bitcoin-hedge-against-inflation.

Makarov, I. and A. Schoar. 2021. Blockchain Analysis of the Bitcoin Market. NBER Working Paper 29396. https://www.nber.org/papers/w29396.

McMillan, R. 2014. The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster. https://www.wired.com/2014/03/bitcoin-exchange/.

Mehrling, P. 2017. Cryptos fear credit. https://sites.bu.edu/perry/2017/09/29/cryptos-fear-credit/.

Möser, M. and R. Böhme. 2015. Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees. In: Brenner, M., N. Christin, B. Johnson and K. Rohloff (eds.). Financial Cryptography and Data Security. FC 2015. Lecture Notes in Computer Science vol. 8976. Springer- Berlin. Heidelberg. https://doi.org/10.1007/978-3-662-48051-9_2.

Mueller, G. 2018. Digital Proudhonism. https://www.boundary2.org/2018/07/mueller/.

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.

Nakamoto, S. 2009. Bitcoin open source implementation of P2P currency. https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1/#selection-69.1-69.216.

Nakamoto, S. 2010. Re: Bitcoins are most like shares of common stock. https://satoshi.nakamotoinstitute.org/posts/bitcointalk/427/#selection-9.0-37.37.

Parkin, J. 2019. The senatorial governance of Bitcoin: making (de)centralized money. Economy and Society 48/4. 483–487.

Pichler, P., A. Schierlinger-Brandmayr and M. Summer. 2018. Digital money. Monetary Policy & the Economy Q3/18. OeNB. 23–35.

Pistor, K. 2019. The Code of Capital. Princeton.

Schuster, E. 2021. Cloud Crypto Land. In: Modern Law Review 84/5. 974–1004.

Shannon, C. E. 1948. A mathematical theory of communication. In: Bell System Technical Journal 27. 379–423. 623–656.

Shiller, R. J. 2020. Narrative Economics: How Stories Go Viral and Drive Major Economic Events. Princeton UP.

Vidan, G. and V. Lehdonvirta. 2018. Mine the gap: Bitcoin and the maintenance of trustlessness. In: New Media and Society 21/1. 42–59. https://doi.org/10.1177/1461444818786220.

Walch, A. 2021. Hearing on Cryptocurrencies: What are they good for? https://www.banking.senate.gov/download/walch-testimony-7-27-21.

Weber, B. 2018. Democratizing Money? Debating Legitimacy in Monetary Reform Proposals. Cambridge UP.

Annex: Glossary of key crypto-related terms[20]

Blockchain: a form of distributed ledger in which details of transactions are held in the ledger in the form of blocks of information. A block of new information is attached into the chain of preexisting blocks via a computerized process by which transactions are validated.

Crypto asset: a type of private sector digital asset that depends primarily on cryptography and distributed ledger or similar technology.

Cryptography: the conversion of data into private code by using encryption algorithms, typically for transmission over a public network.

Distributed ledger technology (DLT): a means of saving information through a distributed ledger, i.e., a repeated digital copy of data available at multiple locations.

Mining: one means to create new crypto assets, often through a mathematical process by which transactions are verified and added to the distributed ledger.

Stablecoin: A crypto asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets, e.g. an official currency.

[20] *Selected from the glossary in FSB (2022).*